Department of Homeland Security
IAIP Directorate
Daily Open Source Infrastructure Report
for 29 August 2003

Current Nationwide Threat Level is

ELEVATED
SIGNIFICANT RISK OF TERRORIST ATTACKS

For info click here
www.whitehouse.gov/homeland

Daily Overview

- The New Haven Register reports that SBC Communications is warning its customers about a phone scam in which imposters try to elicit personal information in the name of the federal government's Do Not Call registry. (See item 7)
- KPUA Hawaii News reports a man who went onto the tarmac at Lihue Airport, threw a rock at a Hawaiian Airlines jet and threatened employees with a knife, was charged yesterday with terroristic threatening, attempted assault, criminal property damage and trespassing. (See item 13)
- The Associated Press reports an investigation into 100 suspicious visa applications has ballooned into one of the nation's largest immigration fraud inquiries, covering as many as 3,500 people cleared to enter the country as religious ministers or multinational executives. (See item 26)
- SearchEnterpriseLinux.com reports that versions 8.12.0 through 8.12.8 of the open−source mail transfer agent Sendmail are vulnerable to remote denial−of−service attacks. (See item 30)
- Internet Security Systems has raised AlertCon to Level 2 due to increased scanning activity for the RealPlayer vulnerability and a confirmed exploit in the wild.

Energy Sector

Current Electricity Sector Threat Alert Levels: Physical: Elevated, Cyber: Elevated
Scale: LOW, GUARDED, ELEVATED, HIGH, SEVERE [Source: ISAC for the Electricity Sector (ES−ISAC) − http://esisac.com]

1. *August 28, Bloomberg News* — **Estimates of stored natural gas are probably too low, U.S. says. The Department of Energy (DOE) said on Wednesday, August 27, that its weekly natural gas inventory reports had probably been underestimating the amount of fuel that utilities were stowing for winter.** The figures have been skewed because the 45 gas storage companies sampled for the weekly report have been more active in tapping and refilling storage than others that were not included in the survey, a DOE statistician, Roy Kass, said. Extrapolating those exaggerated rates to the rest of the industry has been producing incorrect estimates of gas in storage. **The errors were discovered when the weekly estimates were compared with actual inventories reported to the DOE by all 115 U.S. gas storage companies at the end of each month,** Kass said. Speculation that the numbers are erroneous may cause futures prices to fall when the weekly report is released. The department's weekly reports are the primary gauges of demand used by utilities, traders and speculators to predict price movements in the $120 billion gas market in the U.S.
   Source: http://www.nytimes.com/2003/08/28/business/28GAS.html

2. *August 28, ScienceDaily* — **Researchers work to protect power grid from terrorism.** University of Missouri−Rolla researchers developing ways to protect power systems from overloads may also be developing a system to thwart terrorist threats to the nation's power grid. **Electrical engineering professors are working on locally "embedded controllers" that are placed in the electric transmission system to regulate power flow. These FACTS (Flexible AC Transmission System) devices will correct power flow problems and guard against failures.** "Hardware can fail, software can be incorrect and, in the worst case, computers can be taken over by terrorists and set to confuse the FACTS network to do exactly the wrong thing," says Dr. Bruce McMillin, one of the researchers. "Before deploying a FACTS network, these failure and security problems must be addressed. If we can do all of this, we can build and deploy a FACTS network that will be resilient to failure. The results will be to ensure continued power distribution to consumers in the event of failures or attacks."
   Source: http://www.sciencedaily.com/releases/2003/08/030828072723.ht m

3. *August 28, Tucson Citizen (AZ)* — **Southwest Gas Corp.'s equipment again sabotaged. After a seven−month lull, someone again has sabotaged Southwest Gas Corp. equipment in the Tucson, AZ, area − the latest in a three−year series of attacks authorities believe is the responsibility of the same person or people.** The most recent attack came Tuesday, August 26, when someone vandalized a pressure regulator. Tuesday's attack caused an estimated several hundred dollars damage, but did not cause a service outage, according to Ed Scott, an administrative manager with the gas company. **Southwest Gas has been the target of dozens of attacks since November 26, 2000, according to authorities.** Some have knocked out service to limited areas. The attacks mostly have been against equipment that regulates gas pressure in various gas lines in southern Arizona, said sheriff's Detective Jeff Whitbeck, lead investigator on the cases.
   Source: http://www.tucsoncitizen.com/index.php?page=local&story_id=0 82803c1_gassabotage

4. *August 28, BBC News* — **Power cut in London, UK causes chaos. A power outage hit**

London during rush hour at about 6:20 p.m. on Thursday, August 28, and was restored at 7:15 p.m. BST. Between 500 and 1,000 trains were affected by the power cut, thought to have been caused by a problem with the National Grid. South London was hardest hit, and with 60% of the subway and rail network affected. As trains were evacuated, buses quickly became extremely busy and lines of people waiting for taxis grew. Mayor of London Ken Livingstone said at least 100,000 people were affected and said the situation showed the need for a serious look at the National Grid.
Source: http://news.bbc.co.uk/2/hi/uk_news/england/london/3189755.st m

[Return to top]

Chemical Sector

Nothing to report.
[Return to top]

Defense Industrial Base Sector

5. *August 28, Associated Press* — **Fire on nuclear−powered submarine at Norfolk Naval Shipyard injures four. A fire broke out near the nuclear reactor on the USS Florida submarine on Wednesday, August 27, injuring four people slightly but not causing any major damage.** The blaze started just after 10 a.m. and was extinguished in about 10 minutes. Officials say the fire did not damage any of the nuclear−powered submarine's equipment. The submarine's reactor has been shut down for more than two months while the submarine is at the Norfolk Naval Shipyard in Portsmouth, VA, undergoing a major overhaul and conversion. The Navy notified state officials of the fire, the cause of which remained under investigation.
Source: http://www.wavy.com/Global/story.asp?S=1420482&nav=23iiHhWr

6. *August 28, Daily Press (VA)* — **USS Enterprise deployment is a glimpse of the future.** When the USS Enterprise Strike Group departs from the Norfolk Naval Station in Virginia, it will be more than just the first deployment after the Iraqi War. It's a possible preview of the way the Navy will do business for the foreseeable future. The strike group will be composed of five ships instead of the typical 10, and 6,500 sailors instead of roughly 13,000. The deployment length is also changing from the typical six months at sea to as little as three months or as long as eight. **The changes are meant to throw adversaries off by adding elements of flexibility and surprise in naval deployments, and they signal the most significant revamping of carrier operations since the late 1940s,** said Robert Work, a senior defense analyst at the Center for Strategic and Budgetary Assessment. Reasons for the changes can be traced to the war with Iraq. With resources deployed in the Middle East, the military found itself a little undermanned when North Korea started flashing its emerging nuclear arsenal. Defense Secretary Donald Rumsfeld told the services to devise plans to keep the military from getting caught thin again. **The new carrier strike group design is part of the Navy's response. It emphasizes smaller combat elements that can be quickly fitted together to form more powerful ones.**
Source: http://www.dailypress.com/news/local/dp−66274sy0aug28,0,1800 299.story?coll=dp−news−local−final

[Return to top]

Banking and Finance Sector

7. *August 28, New Haven Register (CT)* — **SBC warns of phone scam.** SBC Communications warned its customers on Wednesday, August 27, about a scam involving callers pretending to be customer representatives from the telecommunications company. **The scam artists say they are calling to confirm the customer's participation in the Do Not Call list, a federal program that allows consumers to prevent for−profit telemarketers from calling them at home. The callers ask for personal information such as Social Security number, birth date and mother's maiden name.** The scammers may then use that information to assume the customer's identity and establish a new line of credit or open a telephone account. SBC officials caution customers to question any unusual contact, via phone or e−mail, be careful about revealing personal information, and carefully read all communications from utility and credit card companies.
   Source: http://www.zwire.com/site/news.cfm?newsid=10076363&BRD=1281&PAG=461&dept_id=7546&rfi=6

8. *August 28, Bismarck Tribune (ND)* — **Officials say counterfeit $100 bills show attention to detail. Counterfeit $100 bills circulated in Fargo, ND, and Moorhead, MN, were good forgeries, according to a Secret Service agent. "It's not a bad counterfeit.** Someone put a little effort into making this product," said Brian Snyder, special agent in charge at the Minneapolis office. Cass County, ND, prosecutors charged a Moorhead man on Monday, August 25, with passing counterfeit $100 bills at two Fargo businesses. Moorhead police searched the suspect's home and seized a computer and a floppy disk, according to court records. The court records also show he told police he didn't know the money was counterfeit. **Authorities say about 30 of the bills have turned up in the Fargo−Moorhead area in the past month. Secret Service agents recently inspected specimens, which showed more attention to detail than common forgeries made with computer scanners or color copiers,** Snyder said. The $100 bills likely were made with an offset printer and simulated the tiny red and blue fibers found in authentic currency. However, the portrait and U.S. Treasury seal on the front of the bills were not convincingly faked, he said. Snyder said anyone suspecting a counterfeit bill could easily spot the differences with a magnifying glass.
   Source: http://www.bismarcktribune.com/articles/2003/08/28/news/stat e/sta03.txt

9. *August 28, silicon.com* — **Anti−money laundering banking systems under scrutiny in UK. The Financial Services Authority (FSA), the UK's banking regulator, is asking banks and other financial institutions to share information on the cost and effectiveness of various anti−money laundering techniques, including the automated monitoring of transactions.** The FSA fears that the enforced use of monitoring systems will be too costly and reduce the competitiveness of UK firms. Research by the FSA found that the crackdown on terrorist financing, the scale of many firms' customer base, and advances in technology were drivers for those financial institutions that have adopted anti−money laundering IT systems. But the FSA acknowledges the costs involved may outweigh the potential benefits to both the company and the wider fight against crime.
   Source: http://silicon.com/news/500012/1/5777.html

[Return to top]

Transportation Sector

10. *August 28, WISH−TV (Indianapolis)* — **Airport says many passengers still unprepared for new regulations.** The Indianapolis Airport says plenty of travelers keep arriving unprepared for new security regulations put in place after 9/11. **With Labor Day weekend approaching, the airport wants travelers to check their belongings carefully before boarding an airplane with them.** The Transportation Security Administration, which is now responsible for airport security throughout the country, showed News 8 several items confiscated from passengers at Indianapolis' airport recently. A gun, countless pairs of scissors, sword, knives, baseball bats and even a shoe with razor blades in it were among the items taken away from Indianapolis passengers in the past month. **The TSA says to be prepared to be searched if you're traveling by air. While security has become tighter since 9/11, not all passengers have been quick to adapt to the new rules. The government is reminding passengers to be vigilant and to keep an eye out for someone wanting to do harm on an airplane.**
Source: http://www.wishtv.com/Global/story.asp?S=1421091&nav=0Ra7Hi7 8

11. *August 28, Richmond Times Dispatch* — **Amtrak crash kills truck driver. An Amtrak train struck a dump truck at a railroad crossing in Manassas, VA, Thursday, killing the truck driver and injuring the train's engineer. Authorities said none of the train passengers was injured in the crash.** Amtrak spokesman Dan Stessel said the collision occurred at 9:37 a.m. when the dump truck failed to stop for the train in the community of Broad Run, just outside Manassas. The train was northbound on Amtrak's Crescent run from New Orleans via Atlanta to New York City. **Stessel said the 277 passengers were kept on the train because the location was considered too dangerous to let them off. He said a crane was being sent in to remove the dump truck and one damaged locomotive and that the train would proceed to Washington with the remaining locomotive.** Stessel said the train driver suffered a knee injury and was taken to a hospital, but no passengers were reported injured. The truck driver's identity was not immediately released.
Source: http://www.timesdispatch.com/news/localupdates/MGBT6GP5XJD.h tml

12. *August 28, Associated Press* — **Airport evacuated over spool of wire in landing gear. Authorities evacuated the Great Falls, MT, airport for several hours Thursday morning after one of the pilots of a Delta Air Lines flight found a suspicious object in the plane's landing gear. Airport officials said the object turned out to be spool of wire, possibly left by a maintenance worker.** Peggy Estes, a spokeswoman for Delta in Atlanta, said she could not confirm that, but the incident remained under investigation. **The plane's first officer was doing his preflight check at about 5:45 a.m. when he found the object on the 737−300. Cynthia Schultz, director of the Great Falls International Airport, described it as a cylindrical "package" about 3 inches in diameter and 4 inches long. It was wrapped in white tape and had wires protruding from one end.** Police evacuated the airport terminal and apron, and the FBI and a bomb squad responded. Schultz said officials determined the object was a package of wire commonly used by airline maintenance workers.
Source: http://www.11alive.com/news/usnews_article.aspx?storyid=3595 5

13. *August 28, KPUA Hawaii News* — **Kauai man charged with airport terrorism. A man who allegedly went onto the tarmac at Lihue Airport and threw a rock at a Hawaiian Airlines jet was charged yesterday with a number of offenses. Police say 36−year−old John Meyers of Lihue was charged with terroristic threatening, attempted assault, criminal property damage and trespassing.** Kauai County officials say Meyers climbed over a fence at the north end of the airport shortly after noon Monday and threw a rock at the Hawaiian Air jet. They say he then allegedly threatened employees of both Hawaiian and Aloha airlines with a utility knife before they subdued him. The plane's windshield frame was damaged by the rock. **It was the second armed intrusion at the airport in the past three months. In May, Lloyd Albinio allegedly broke into the airport terminal through the baggage claim area, pointed a pistol at a federal security officer and fired two shots inside the airport.**
Source: http://www.kpua.net/news.php?id=540

14. *August 28, Today* — **Truck maker says fleets concerned over security. A survey conducted by International Truck & Engine stresses the fleet community's concern with security requirements in the aftermath of 9−11.** According to International, some 70 per cent of North American fleet managers responding to a monthly survey on the company,s web site said they are "very" or "somewhat" concerned about cargo and vehicle security. About 56 per cent said hazardous materials haulers face higher than normal security risks; over 50 per cent cited agriculture and food distribution, 44 per cent regional and long−haul operations. **In a recent white paper, "Homeland Security: Implications for the truck and School Bus Industry," International says that measures in place or being considered by the federal government will have the greatest affect on hazardous cargo, intermodal, trans−border, food and agriculture and school bus operations.** International and other truck manufacturers will have to deliver the technological infrastructure to support many of the security systems in use or on the drawing boards, says Jeff Bannister, director, truck electronics. Wireless technologies are key to a number of security solutions, says Bannister.
Source: http://www.todaystrucking.com/displayarticle.cfm?ID=2625

15. *August 27, Federal Computer Week* — **Air traffic system debuts in Florida. The first deployment of an automated air traffic system was completed yesterday, August 27, marking a significant improvement in the direct routing of aircraft.** The new software eases the burden on air traffic controllers by predicting potential conflicts with other aircraft up to 20 minutes in advance. It can also determine if pilot−requested changes to a flight plan are free of conflicts with other aircraft. **The system continuously monitors aircraft in comparison to their flight plans and issues a controller alert 40 minutes before an aircraft is predicted to enter restricted or prohibited airspace.** All of the FAA's 14 centers nationwide should have the software operational by 2005, federal officials said.
Source: http://www.fcw.com/fcw/articles/2003/0825/web−faa−08−27−03.a sp

[Return to top]

Postal and Shipping Sector

Nothing to report.
[Return to top]

Agriculture Sector

16. *August 28, CottonWorld* — **Integrated assault on fusarium in cotton. Modification of standard cotton crop management practices can produce better control of fusarium wilt, according to plant pathologist Stephen Allen.** Allen said a suite of strategies are now available that could provide more positive results. He said it was well recognized that the fusarium pathogen survived on crop residues, and could increase and multiply if crop residues are incorporated in the soil. **He quoted two trials, including one where the cotton crop residues were left on top of beds for 6−8 weeks prior to incorporation, reducing the impact of the disease and boosting plant survival in the crop by more than 30 percent.** "Rotations are also a problem. **We've done experiments over a couple of seasons now comparing a bare fallow with growing a cereal and incorporating those residues back into the beds. Survival has been 20 percent higher after a bare fallow than after a cereal rotation where we have incorporated the residues," he said.** He acknowledged that bare fallow rotations are not always the most desirable option, other options are also under investigation including burning the cereal residues; allowing the cereal residues to stand and be weathered before incorporation; and leaving the cereal residue standing throughout the season. Source: http://www.cottonworld.com.au/articles.php3?rc=571

17. *August 27, Canadian Press* — **Russia says it will accept Canadian beef. Russia has agreed to open its borders to imports of boneless Canadian beef from animals of any age, provided the cattle can be proven free of contact with bovine spongiform encephalopathy (BSE).** The move was announced Wednesday by the Canada Beef Export Federation, which says it received notification from the Canadian Food Inspection Agency. "Russia is the first country that has clearly moved independently from the U.S. in stating what their expectations are for animals over 30 months of age," said Ten Haney, president of the export federation. **Boneless beef from animals 30 months of age or less, which are believed too young to develop the disease, must be certified to come from animals born and raised in Canada. They must originate from farms which have never recorded a case of BSE. Animals over 30 months of age must be tested and found free of BSE.** Haney said the testing costs could be between $25 and $100 per animal and could depend on the scale of testing. It's not known if the tests would have to be done by federal food inspectors. **Any Canadian slaughterhouses and meat−packing plants exporting to Russia must be pre−approved by the Russian veterinary authority. Haney expects that process to take about six weeks.** Source: http://www.canada.com/ottawa/story.asp?id=662BF480−CD3A−4B97−B068−6C2E04D86EF1

18. *August 27, Associated Press* — **Industry struggles with biotech corn. Seed companies, farmers, and grain handlers are struggling with how to keep genetically altered corn from mixing with non−biotech crops.** There is no simple way to ensure that biotech varieties go only where they're accepted. Some safeguards are already in place, but the process is still evolving. Some in the industry say changes aren't happening fast enough to keep up with the steadily increasing use of genetically altered crops. They fear problems similar to what happened with StarLink in 2000, when the biotech corn not approved for human consumption was accidentally mixed with other crops. The resulting scare triggered food recalls and caused a worldwide drop in corn prices. **More biotech corn is being planted each year in the U.S., with 40 percent of the corn this year being genetically altered.** That was up from about

one−third of all corn planted last year. **Any co−mingling of grain, however small, headed for a country that won't accept it endangers the entire shipment, said Peter Goldsmith, an assistant professor at the University of Illinois' College of Agriculture. At least seven biotech corn varieties have not been approved for use in the European Union.**
Source: http://www.washingtonpost.com/wp−dyn/articles/A52251−2003Aug 27.html

[Return to top]

Food Sector

Nothing to report.
[Return to top]

Water Sector

19. *August 28, New York Times* — **Sewage spill exposes a lingering problem. Minutes after New York City lost its power on August 14, raw sewage began to flow into surrounding waterways.** By the time electricity was restored, 490 million gallons had spilled. This was not the first time. The blackout of 1977 caused a sewage overflow of 828 million gallons, which spilled from eight treatment plants. Back then, city officials found a solution: they provided all treatment plants with backup generators, which functioned properly, for the most part, during the blackout earlier this month. But no generator was ever built at the 13th Street Pump Station. **"We always knew if there was a blackout, 13th Street would just shut its gates and pump everything out," said Alfonso R. Lopez, deputy commissioner for the Bureau of Waste Water Treatment. "Everybody recognizes we need generators. No one wants to give up real estate." To be sure, this was not the only sewage problem on August 14. More than 260 million gallons of raw sewage was spilled because of faulty or inoperable generators at 2 of the city's 14 waste water treatment plants.** And even if those generators had been running properly and the 13th Street station had had backup power, sewage would still have spilled because of the lag time before generators begin operating, Lopez said.
Source: http://www.nytimes.com/2003/08/28/nyregion/28SEWA.html

20. *August 28, Beacon Journal* — **Akron waterlines nearly went dry. Akron, OH came within an hour of not being able to deliver water to any of its customers last weekend when an equipment failure triggered a flood at a water treatment plant.** Getting the water flowing again would have been far more inconvenient than the 29−hour citywide boil alert later implemented. As employees and volunteers worked through the night Sunday to pump more than a million gallons of water from the plant's flooded basement, the city's two reserve storage tanks slowly were being drained, with one tank dropping from its usual, 30−foot−high water level to 1 ½ feet. Those tanks provide the critical pressure that keeps the system working, even if the water plant is shut down. Without that pressure, there isn't enough push to get water into homes and businesses, airlocks can develop in the lines, and there can be backflow that would contaminate the entire system. **The near miss was one of the consequences after a valve failure in the plant that led to millions of gallons of water backing up in the plant's basement instead of flowing into the system. Michael McGlinchy, manager of the Public Utilities Bureau, said that the breakdown highlights the vulnerability of a system that**

pumps 50 million gallons of water daily to 300,000 customers in several communities.
Source: http://www.ohio.com/mld/ohio/news/6636825.htm

[Return to top]

Public Health Sector

21. *August 28, Associated Press* — **CDC: West Nile doubles again.** West Nile virus activity has again doubled, now affecting more than 1,400 people in the United States, federal officials said Wednesday. **Thirty−four states reported a total of 1,442 cases and 21 deaths, the U.S. Centers for Disease Control and Prevention (CDC) said. Last week, the agency reported 715 cases and 14 deaths.** Colorado and the central United States continue to be the hardest hit. Colorado's 635 human cases lead the country, followed by 204 cases in South Dakota, 190 in Nebraska and 106 in Texas, the CDC said. Six of the country's deaths were in Colorado, followed by four in Nebraska.
Source: http://www.canada.com/health/story.html?id=51F572C0−21F7−4E26−9E58−D8E73DFBA17D

22. *August 28, South Florida Sun−Sentinel* — **Malaria experts consider outbreak localized. The malaria outbreak in Palm Beach, FL, looks like a localized cluster of cases that can be halted in a fairly short time, showing no signs of a widespread, lingering infestation, a federal malaria expert said Wednesday. The next month or so will tell whether the mosquito−borne disease will fade away, as has occurred in almost all U.S. outbreaks, or whether it will gain a foothold in the mosquito pool and become a longer−term threat, the expert said.** "There's no magic way to tell. It's watching the pattern and watching the trend," said Louise Causer, a malaria specialist at the U.S. Centers for Disease Control and Prevention (CDC). **The seven cases among people living west of Lake Worth since July 27 constitute the nation's largest single outbreak of locally contracted malaria since a rash of 27 cases in California in the mid−1980s, the CDC says.** That one lasted several months, Causer said. Telltale signs of a lingering infestation: If people get sick far from the original cluster. If new cases arise for another month, after intensive spraying. If mosquitoes caught in traps test positive for malaria. "None of those have happened," Causer said. "It's reassuring that those things are not out of control."
Source: http://www.sun−sentinel.com/news/local/southflorida/sfl−rxmalar28aug28,0,2211322.story?coll=sfla−home−headlines

23. *August 27, Reuters* — **Half of U.S. smallpox doses shipped. The British pharmaceutical company, contracted by the United States to supply smallpox vaccine, said on Wednesday it had made and tested all 155 million doses and delivered over half to the U.S. stockpile. The company said the remaining vials would be handed over in the coming weeks after discussions with U.S. regulators over labelling.** Fears of biological attack have persuaded governments to build up stocks of smallpox vaccine to protect the population. Scientists believe smallpox, a highly contagious disease that leads to fever and blistering and kills around 30 percent of its victims, could blow up into a worldwide plague. It was eradicated in 1979, but the U.S. government and some experts believe some governments and groups may have developed the virus for use as a biological weapon.
Source: http://asia.reuters.com/newsArticle.jhtml?type=healthNews&storyID=3346243

24. *August 26, Associated Press* — **Seven health workers with flu−like symptoms checked for SARS. A Hong Kong public hospital quarantined 24 patients after seven of its health workers developed flu−like symptoms, although none have tested positive for Severe Acute Resiratory Syndrome (SARS), officials said Wednesday.** Five nurses and two health care assistants working in a ward at the Alice Ho Miu Ling Nethersole Hospital in suburban Tai Po developed symptoms such as coughs, sore throats and fevers on Friday, hospital spokeswoman Ellen Wong said. Five of the health workers have returned to work while two were on sick leave, Wong said. The 24 patients have been barred from leaving since Monday and are being monitored for SARS after some developed mild fevers and coughs, Wong said. **Health Department spokeswoman Eva Wong said preliminary evidence showed the cases were not related to SARS.**
Source: http://famulus.msnbc.com/FamulusIntl/ap08−26−201812.asp?reg= PACRIM

[Return to top]

Government Sector

25. *August 28, Click10.com* — **ICE makes major bust on Miami River. Immigration and Customs Enforcement (ICE) agents and U.S. Customs and Border Protection inspectors announced the seizure of 486 pounds of cocaine that was concealed in two hidden compartments between the fuel tanks of the cargo ship MS Lyly 1. The 184−foot Lyly 1 arrived on the Miami River August 16 from Port au Paix, Haiti, and had been searched previously.** The previous searches by inspectors and information developed by ICE agents led last night's team to the machinery areas of the ship including the engine room. At about 8 p.m., inspectors searching the engine room drilled a hole into the deck. When they removed the drill bit, it was covered with a white powdery substance that tested positive for cocaine. The ship's crew members (one Peruvian, one Cuban, two Haitians and two Hondurans) were interviewed throughout the night. No arrests have been made at this time. **ICE agents will begin an investigation into who shipped the cocaine and where it was to be delivered.**
Source: http://www.click10.com/news/2441287/detail.html

26. *August 28, Associated Press* — **Probe of Miami lawyer balloons into massive visa fraud case. An investigation into 100 suspicious visa applications has ballooned into one of the nation's largest immigration fraud inquiries, covering as many as 3,500 people cleared to enter the country as religious ministers or multinational executives.** Immigration officials outlined their discoveries Thursday at the sentencing of immigration lawyer Javier Lopera. He was ordered to spend eight years and four months in federal prison and faces deportation afterward. **Through Lopera's visa mill, prosecutor Ben Daniel said virtually an entire Brazilian slum was authorized to enter the United States legally. Investigators found as many as 450 cleaners posing as ministers, and only one legitimate request has been approved in 500 applications subjected to extensive review after charges were filed.** "It wasn't about all money. It was about arrogance of getting something through the system," said investigator Ronnie Thomas, who has devoted two years to Lopera's scams. "He had his money coming in, but he loved the challenge." **The probe uncovered 3,500 people listed by Lopera on 7,000 suspicious applications dating back to 1996. The investigation and a review of the suspect cases will cost an estimated $1.8 million. "We have not encountered any type of**

fraud of this magnitude at the service center before," testified Veronica Traylor, an acting assistant director of the Dallas center of the U.S. Bureau of Citizen and Immigration Services.
Source: http://www.sun−sentinel.com/news/local/southflorida/sfl−828visalawyer,0,3171439.story?coll=sfla−home−headlines

[Return to top]

Emergency Services Sector

27. *August 28, eSecurity Planet* — **Partnership aims to accelerate Homeland Security tech adoption. Recently launched in Oregon, the Regional Alliances for Infrastructure and Network Security (RAINS) is a partnership of private industry and public agencies is an effort to accelerate development and deployment of innovation technology for homeland security.** With over 60 technology supporters and 300 participating organizations including universities and public safety agencies, RAINS−Net is linking 911 emergency response centers with local public safety stakeholders such as schools, hospitals and office buildings. For example, if police are dispatched to someone threatening with a gun in the neighborhood of a school, the school principal is notified that the incident is in progress. **The key technology innovation was to link the computer−aided dispatch system used within the 911 centers, a legacy system that is essentially not interoperable, into a XML and Web services format that can be easily integrated to the outside world.** The price for municipalities to participate in RAINS−Net is likely to be in the $500,000 to $2 million range, depending in the number of servers and how much information sharing is required.
Source: http://www.esecurityplanet.com/trends/article.php/3070021

[Return to top]

Information and Telecommunications Sector

28. *August 28, Washington Post* — **Fight against viruses may move to servers. Computer viruses are becoming so aggressive and sophisticated that they may soon be able to elude anti−virus programs installed on individual computers**, according to many in the security industry. Analysts say **the speed with which viruses and worms now propagate require technologies that predict outbreaks before they happen. Such predictive systems require intensive computing power beyond the capacity of desktop machines**. Computer worms and viruses are getting more sophisticated, are spreading faster and are capable of doing more damage than those of the past. Viruses such as Sobig.F can change during their attacks by receiving updates and new instructions from other computers. Some analysts point out that while no software or hardware is perfect, it's much easier to spread viruses when so much of the computing world depends on the Microsoft Windows operating system. Advocates of the Unix, Linux, Macintosh and other operating systems argue that they are more secure than Windows, but others note that those systems simply have not been targeted as much.
Source: http://www.washingtonpost.com/wp−dyn/articles/A56103−2003Aug27.html?referrer=email

29.

August 28, Federal Computer Week — **North Carolina agency expands Internet mandate. North Carolina's Rural Internet Access Authority (RIAA) will be able to develop high−speed Internet access in urban areas statewide, beginning next year**. Gov. Michael Easley recently signed into law a measure that extends the public/private RIAA's mandate for another three years beginning January 2004, under the control of the newly created e−NC Authority. Established telecommunications companies show the same reluctance to provide high−speed services in poor urban areas as they have in remote rural areas, said Jane Patterson, executive director of the authority, and wireless is often the only technology the RIAA has had available to provide those services quickly. But their access needs can't be addressed under the current authority, she said. **The e−NC Authority will also begin using the Federal Communications Commission's definition of high−speed access to set the floor level for Internet services in rural and urban areas**. "The companies are trying to get even lower speeds into the law," Patterson said. "In the [statute setting up the RIAA] 128 kilobits/sec is the definition of high speed, whereas we actually have 384 kilobits/sec access everywhere now." FCC guidelines use 200 kilobits/sec or more in both uplink and downlink directions as the basis for defining high−speed access.
Source: http://fcw.com/geb/articles/2003/0825/web−nc−08−28−03.asp

30. *August 27, SearchEnterpriseLinux.com* — **Sendmail vulnerable to DoS attacks. Versions 8.12.0 through 8.12.8 of the open−source mail transfer agent Sendmail are vulnerable to remote denial−of−service attacks**, according to an alert issued by the FreeBSD Project. The vulnerability is in the code that implements DNS (domain name system) maps. An attacker sending a malformed DNS reply packet could cause Sendmail to call "free ()" on an uninitialized pointer. Such a call could cause a Sendmail child process to crash. Sendmail is widely implemented in enterprises as part of several Linux and Unix distributions. **A patch is available on the Sendmail Website**: http://Sendmail.org/dnsmap1.html
Source: http://searchenterpriselinux.techtarget.com/originalContent/0,289142,sid39_gci921467,00.html

31. *August 27, eSecurity Planet* — **ISSA seeks to define generally accepted security principles.** The Information Systems Security Association (ISSA), which has 10,000 security professionals as members in 100 countries, has issued a global call for volunteers to participate in the development and maintenance of the Generally Accepted Information Security Principles (GAISP). **The GAISP aims to be a comprehensive guide to security standards and practices, and will fulfill a third level of effort since activity to define standard security principles**. The first two levels are the Pervasive Principles, which target top executive leadership of organizations, and Broad Functional Principles, which targets IT management. The third level, Detailed Principles, is intended to address the day−to−day security measures needed to fulfill the other two levels. The Detailed Principles will be derived from a review and cross−referencing of existing guidance and standards materials. "For years we have had the Generally Accepted Accounting Principles to guide the financial reporting process, but we have not had something similar for information security," says Mike Rasmussen, chairman of the GAISP effort. **The goal is to produce a framework that security professionals can use to see where regulations overlap and where they differ**. Additional information is available on the ISSA Website: www.issa.org/gaisp.html
Source: http://www.esecurityplanet.com/trends/article.php/3069541

Internet Alert Dashboard

Current Alert Levels

 AlertCon: 2 out of 4 https://gtoc.iss.net	 Security Focus ThreatCon: 2 out of 4 http://analyzer.securityfocus.com/

Current Virus and Port Attacks

Virus:	#1 Virus in the United States: **WORM_SOBIG.F** Source: http://wtc.trendmicro.com/wtc/wmap.html, Trend World Micro Virus Tracking Center [Infected Computers, North America, Past 24 hours, #1 in United States]
Top 10 Target Ports	135 (epmap), 1434 (ms−sql−m), 137 (netbios−ns), 4899 (radmin), 445 (microsoft−ds), 80 (www), 1433 (ms−sql−s), 139 (netbios−ssn), 27374 (SubSeven), 554 (rtsp) Source: http://isc.incidents.org/top10.html; Internet Storm Center

[Return to top]

General Sector

32. *August 28, Associated Press* — **Three small blasts near Chiron plant in Emeryville. Three explosions jarred Emeryville, CA, on Thursday, August 28, at the headquarters of Chiron, an international pharmaceutical research firm.** Authorities say the first bomb went off around 3 a.m. and the second at 4 a.m. outside of the facility. The third blast, shortly before 7 a.m., was the Alameda County, CA, bomb squad detonating a suspicious package found near the facility. The package turned out to be harmless. No claim of responsibility has been reported.
Source: http://www.bayarea.com/mld/mercurynews/news/local/6639294.ht m

[Return to top]

DHS/IAIP Products &Contact Information

The Department of Homeland Security's Information Analysis and Infrastructure Protection (IAIP) serves as a national critical infrastructure threat assessment, warning, vulnerability entity. The IAIP provides a range of bulletins and advisories of interest to information system security and professionals and those involved in protecting public and private infrastructures. By visiting the IAIP web−site (http://www.nipc.gov), one can quickly access any of the following DHS/IAIP products:

DHS/IAIP Warnings − DHS/IAIP Assessements, Advisories, and Alerts: DHS/IAIP produces three levels of infrastructure warnings. Collectively, these threat warning products will be based on material that is significant, credible, timely, and that address cyber and/or infrastructure dimensions with possibly significant impact.

DHS/IAIP Publications − DHS/IAIP Daily Reports, CyberNotes, Information Bulletins, and other publications

DHS/IAIP Daily Reports Archive − Access past DHS/IAIP Daily Open Source Infrastructure Reports

DHS/IAIP Daily Open Source Infrastructure Report Contact Information

Content and Suggestions:	nipcdailyadmin@mail.nipc.osis.gov or contact the DHS/IAIP Daily Report Team at (703)883−6631
Subscription and Distribution Information	Send mail to nipcdailyadmin@mail.nipc.osis.gov for more information.

Contact DHS/IAIP

To report any incidents or to request information from DHS/IAIP, contact the DHS/IAIP Watch at nipc.watch@fbi.gov or call (202)323−3204.

DHS/IAIP Disclaimer